REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed on February 27, 2004 ("Office Action"). Claims 1-34 were rejected. In this Amendment, claims 1, 3, 4, 16, 19, 25-27 and 33 have been amended. Claims 1-34 are pending in the application.

Interview Summary

Applicants thank the Examiner for the courtesy to Applicants in granting an interview to discuss the application. In the interview, Applicants reviewed differences between the reference U.S. Pat. No. 6,070,244 (Orchier) and claim 1. Applicants pointed to the lack of several items in Orchier as discussed herein such as event objects and broadcasting intrusion information in real time. The Examiner pointed to sections of Orchier as discussed in the Examiner's Interview Summary. However, Applicants did not agree with the Examiner's interpretation of Orchier, nor its application to the claims.

In particular, the Examiner pointed to Orchier, column 13, line 11-13 for a teaching of "real time." Applicants explained that the cited section of Orchier teaches an alert agent that automatically notifies appropriate personnel of particular conditions, but that Orchier does not teach the real time approach of the invention as claimed in claim 1. Applicants explained, as detailed below, that the automatic notification is not the claimed real time approach and that in fact Orchier teaches actions at scheduled intervals, which contradicts the real time approach of claim 1.

Defective Oath/Declaration

Applicants do not agree with the objection to the declaration because the declaration of February 10, 2004 was a supplemental declaration, and the Patent Rules provide that "[d]eficiencies or inaccuracies relating to fewer than all of the inventor(s) or applicant(s) (citations omitted) may be corrected with a supplemental oath or declaration identifying the entire inventive entity but signed by only the inventor(s) or applicant(s) to whom the error or deficiency relates." 37 U.S.C. § 1.67(a)(2) (emphasis added).

However, current herewith, Applicant provides an *Amendment, Petition And Fee To Delete And/Or Add To Original Erroneously Named Or Not Named Inventor(s) In Declaration – Nonprovisional Application – (37 C.F.R. §1.48(a))* to correct inventorship with a new oath with

signatures from all the inventors. It is thus believed that the objection has been overcome in any event. Removal of the objection is therefore respectfully requested.

Rejection of Claims 16 and 20 under 35 USC § 112, Second Paragraph

Claims 16 and 20 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. The Office Action referred to lack of antecedent basis in claims 16 and 20. Claim 16 has been amended, and claim 19, from which claim 20 depends, has been amended. It is now believed that the rejection with respect to antecedent basis has been overcome. Review and approval are respectfully requested.

Objection to Claim 20

The Office Action objected to claim 20 with respect to a misspelling. However, it is believed that the misspelling was present in claim 27, rather than claim 20, and claim 27 has been amended to correct a misspelling objected to in the Office Action. Accordingly, this objection is believed overcome. Review and approval are respectfully requested.

Rejection of Claims 1-10, 12-15, 17-22, 25-31, 33 and 34 under 35 USC § 102(e)

Claims 1-10, 12-15, 17-22, 25-31, 33 and 34 were rejected under 35 USC § 102(e) as being anticipated by U.S. Pat. No. 6,070,244 (Orchier). Applicants respectfully traverse the rejection.

Claims 1 and 25 have been amended to expedite allowance of the application. However, it is believed that such amendment is not necessary in view of the cited art. Applicants reserve Applicants' right to pursue such claims in their unamended form in a continuation application.

It is believed that the rejection in view of Orchier should be removed. As stated above, in the interview, the Examiner pointed to Orchier, column 13, line 11-13 for a teaching of "real time." However, Applicants do not believe that this cited portion of Orchier or Orchier generally supports the claimed real time aspects of claim 1. The cited section of Orchier teaches an alert agent that automatically notifies appropriate personnel of particular conditions. Automatic notification is not equivalent to the real time actions claimed in claim 1. It is possible that actions may take place automatically, that is, without human intervention, while at the same time not taking place in real time. In fact Orchier teaches actions at scheduled intervals. See for example, Figures 4b, 4c, and 4e of Orchier, which refer to actions taking place at a designated

time of day. Thus, Orchier is teaching a batch approach, rather than a real time approach. See also Orchier, column 11, lines 4-6, which refer to steps including scheduling the starting of the program at a designated time of day.

In the Interview Summary, the Examiner indicates that the Examiner is "interpreting this process consisting of real time to the appropriate individuals who need to be informed of the intrusions," with respect to automatic notification disclosed in Orchier. However, Applicants do not believe that Orchier discloses the real time approach in the way claimed in claim 1. Claim 1 includes "the event parser being able to receive log data in real time from the device," and the "event broadcaster being able to transmit the event object in real time, relative to the receipt of the log data, as an intrusion alarm." Therefore, even if the Examiner's interpretation were correct, there is still no disclosure in Orchier of the real time aspects of both the event parser and event broadcaster and the interaction between these elements.

As noted above, Orchier teaches a batch approach. Additionally, Applicants point the Examiner to Orchier, column 13, lines 4-7. This indicates that the alert agent analyzes collected data residing in a database. Thus, Orchier is referring to actions with respect to collected data, rather than teaching "the event parser being able to receive log data in real time from the device," and the "event broadcaster being able to transmit the event object in real time, relative to the receipt of the log data, as an intrusion alarm." Therefore, Orchier does not teach an event parser that receives log data in real time, in communication with an event manager that designates an event object to be broadcast in real time, in communication with an event broadcaster that is able to transmit the event object in real time, relative to the receipt of the log data. Thus, even if some actions in Orchier take place automatically, Orchier does not teach the particular real time approach of claim 1.

Further, claim 1 has been amended to add "relative to the receipt of the log data," so that claim 1 now includes "an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object in real time, relative to the receipt of the log data, as an intrusion alarm." Such amendment was made to clarify the meaning of real time in claim 1. Column 13, lines 4-7 of Orchier refer to automatic notification with respect to collected data residing in a database. Thus, Orchier is teaching automatic notification based on collected data

residing in a database, not to receiving log data in real time from a device and transmitting an event object in real time, relative to the receipt of the log data.

Thus, it is believed that the invention as claimed in claim 1 is not taught or suggested by the reference Orchier and the rejection should be removed. Below are some additional reasons that it is believed that the application of Orchier to claim 1 is incorrect.

For example, the Office Action points to column 4, lines 5-10 of Orchier regarding an event parser being able to parse information to create a corresponding event object. See Office Action at 4. However, the cited portion of Orchier does not refer to creation of event objects. The cited portion of Orchier indicates:

> . . . 1) are all coupled to an abstraction facility 54 which serves to reformat and standardize security related data packets. Thereby, the abstraction facility 54 is able to provide over line 55 security data pertaining to all of the subsystems 12-20 for the purpose of being handled by the central security processor 60 in a consistent and standard manner.

Orchier, column 4, lines 5-10. There is no discussion or disclosure of event objects in the cited portion of Orchier. Thus, Orchier fails to teach an event parser being able to parse information to create a corresponding event object corresponding to the intrusion event. Applicants do not find support for the Examiner's interpretation of a teaching of this in Orchier as the Examiner states in the Interview Summary.

Also regarding claim 1, the Office Action cites Orchier column 4, lines 10-21 for an event manager, the event manager designating the event object to be broadcast in real time. Office Action at 4. It is believed that such interpretation of Orchier is incorrect. The cited portion of Orchier states:

> . . . security processor 60 in a consistent and standard manner. This enables a security administration or personnel 62 which is coupled to the central security processors 60 to handle and deal with security issues in a direct, globally applicable and standardized format. Indeed, the central processor is programmed to act on many security related decisions automatically. Either way, when a decision concerning security matters is made, the processor responds by taking several actions, including providing relevant information and commands to a compliance facility 58 which process the information and causes the central security processor 60 to issue the appropriate commands to the local commands translator 56.

Orchier, column 4, lines 10-15. The cited portion of Orchier does not, for example, refer to broadcast of an event in real time. The cited portion of Orchier also does not refer to a predetermined threshold condition.

Also regarding claim 1, the Office Action cites Orchier, column 4, lines 27-30 regarding an event broadcaster, the event broadcaster being able to transmit the event object in real time as an intrusion alarm. Office Action at 5. The cited portion of Orchier does not appear to refer to such teaching. The cited portion of Orchier merely states:

> The compliance facility 58 also interfaces with an alerting facility agent 64 that is able to contact key personnel or other computer systems, e.g. an external system 68, regarding security breaches. Appropriate hard copy reports and the like can be provided through a reports generator 66.

Orchier, column 4, lines 27-30. This cited portion fails to provide a teaching in Orchier of an event broadcaster being able to transmit the event object in real time as an intrusion alarm. The cited portion may refer to batch processing that does not take place in real time. Such an approach may be consistent with the indication that appropriate hard copy reports are provided. For example, Orchier, column 11, lines 4-6, refers to steps including scheduling the starting of the program at a designated time of day.

Thus, a number of reasons have been discussed each of which would be sufficient reason for removal of the rejection of claim 1. Therefore, it is believed that claim 1 is patentable over the cited references, and removal of the rejection is respectfully requested.

Claims 2-24 depend directly or indirectly from claim 1 and are believed patentable for at least the reasons as to claim 1. Further, these claims are believed independently patentable, and it is believed that the application of Orchier to such claims as provided in the Office Action is incorrect.

For example, with respect to claims 4 and 27, the Office Action refers, inter alia, to column 4, lines 5-10 regarding means for transmitting log data having a conforming message format to event parses, said means being coupled to a network port. Office Action at 6. Column 4, lines 5-10 of Orchier, provide the following:

> . . . 1) are all coupled to an abstraction facility 54 which serves to reformat and standardize security related data packets. Thereby, the abstraction facility 54 is able to provide over line 55 security data pertaining to all of the subsystems 12-20 for the purpose of being handled by the central security processor 60 in a consistent and standard manner.

Orchier, column 4, lines 5-10. Such portion of Orchier fails to mention a network port or provide any teaching or suggestion of means for transmitting log data having a conforming message format to event parsers, said means being coupled to a network port. Thus, it is believed that the rejection as to claims 4 and 27 should be removed at least for this reason.

As to claim 6, the Office Action cites Orchier column 14, lines 5-10 and Fig. 8b regarding a graphical user interface screen comprising an alarm console coupled to an event broadcaster, configured to display intrusion alarms, and a report console configured to execute queries input by user and display results, wherein the alarm console and event broadcaster are displayed simultaneously on the display screen. Office Action at 7 (emphasis added). Such portion of Orchier provides:

> [a user interface that operates in accordance] with the flow-chart of Fig. 9a. Such a user interface may comprise a search screen 86a, a list of accounts screen 86b, a single account detail screen 86c, an account updating screen 86d and such other screens as are necessary to provide full and effective communication by users of the system.

Orchier, column 14, lines 5-10. Such portion of Orchier does not teach an alarm console or the simultaneous display of an alarm console and event broadcaster on a display screen. Thus, it is believed the rejection of claim 6 should be removed, and such action is respectfully requested.

As to claims 7 and 30, the Office Action cites column 13, lines 45-50 and Fig. 8b, "Note" for teaching a report console further configured to display query result data and summary lines, said summary lines comprising hypertext links providing access to further data. Office Action at page 7 (emphasis added). The cited text of Orchier, column 13, lines 45-50 does not appear to teach such an approach including hypertext links providing access to further data. Rather, such portion of Orchier provides:

> [Both] standard and ad-hoc queries are supported by the software implementation of the agent 82. The query agent 82 has been reduced to practice in a form that uses an Internet/Intranet technology, i.e. a web browser, to allow access with a minimum of connectivity and software distribution problems. Any query tools that handles Sybase™ could be used [in the implementation.]

Orchier, column 13, lines 45-50. The use of Internet/Intranet technology, i.e., a web browser, as disclosed in Orchier fails to teach the particular use of summary lines comprising hypertext links providing access to further data. Such teaching of such a particular approach is not present in the general discussion of Internet/Intranet technology or a web browser. Thus, it is believed the

rejection with respect to claims 7 and 30 should be removed, and such action is respectfully requested.

Claims 8 and 29 were rejected based on a similar interpretation of Orchier with respect to column 13, lines 45-50 and Fig. 8b. It is therefore believed that the rejection of such claims should also be removed.

Claim 9 was rejected citing column 2, lines 30-35 Orchier for teaching a graphical user interface displaying the status of network security devices in real time. Office Action at 7. It is believed that such interpretation of Orchier is incorrect. The cited portion of Orchier, provides:

> The technology independent layer handles the main functionality of the system: locating terminating employees, auditing system and user data, monitoring security events (e.g. failed login attempts), automatically initiating corrective action, interfacing with the system users, reporting, querying and storing of collected data.

Orchier, column 2, lines 30-35. Such description fails to teach a graphical user interface displaying the status of network security devices in real time. In fact, the cited portion of Orchier is directed to a layer of a layered software architecture. The cited portion is related to a technology independent layer of the software. This general discussion fails to teach a graphical user interface to explain the status of network security devices in real time.

Claims 12, 33 and 34 were rejected based on a citation of Orchier, column 13, lines 10-15 and column 14, lines 5-10, for a teaching of a chat manager accessible to a user from an alarm console for executing electronic communications links between the user and others having an electronic communication link to the computer system. Office Action at 8. The cited description of Orchier fails to teach a chat manager. The cited portion of Orchier provides:

> . . . of certain key security or operating system files within any one of the security domains 70a-70n. The alert agent 80 automatically notifies appropriate personnel by e-mail, phone and/or pager. This is indicated by the alarm arrow 81 in Fig. 3b. The alert agent 80 is unique in that it is able to monitor across dissimilar environments, ...

Orchier, column 13, lines 10-15. Applicants fail to find any teaching of the chat manager. A chat manager does not follow from teaching of notification by email, phone and/or pager. Therefore, it is believed that the rejection of claims 13, 33 and 34 is in error and should be removed. Such action is respectfully requested.

As to claim 25, the Office Action cites, inter alia, Orchier, column 13, lines 10-12 for broadcasting an event object as an intrusion alarm in real time to a display screen on a graphic user interface. Such portion of Orchier indicates:

> [modifica]tion of certain key security or operating system files within any one of the security domains 70a-70n. The alert agent 80 automatically notifies appropriate personnel by e-mail, phone and/or pager. This is indicated by the alarm arrow 81 in Fig. 3b.

Orchier, column 13, lines 10-12. It is believed that such description fails to teach broadcasting an event object as an intrusion alarm in real time to a display screen on a graphic user interface. There is no discussion of an event object in the cited portion of Orchier. There is also no discussion of broadcasting an event object as an intrusion alarm in real time to a display screen on a graphic user interface. There is merely a discussion of an alert agent automatically notifying personnel by email, phone and/or pager. Such discussion does not require a graphic user interface, nor does such discussion teach broadcasting of an event object. Also, as discussed above, it is not believed that the cited portion of Orchier teaches the claimed real time approach. Thus, it is believed that the Office Action is in error and that the rejection should be removed, and such action is respectfully requested.

Claim 25 also refers to intrusion events from log data received from network services devices in a computer network. In particular, claim 25, as amended, indicates that the network services devices comprise a device from a group comprising a firewall, VPN (virtual private network) server or router, and e-mail server. Orchier does not provide teaching or suggestion of handling of network intrusion events from log data received from network services devices as claimed in claim 1. For this additional reason, it is believed that the rejection of claim 1 should be removed.

Claims 26-34 depend from claim 25 and are thus patentable for at least the reasons of claim 25. It is also believed that such claims are independently patentable. Thus, removal of the rejection of such claims is respectfully requested.

Rejection of Claims 11, 16, 23, 24 and 32 under 35 USC § 103(a)

Claims 11, 16, 23, 24 and 32 were rejected under 35 USC § 103(a). Applicants respectfully traverse the rejection. Such claims depend directly or indirectly from claims that are believed patentable for the reasons discussed above. Therefore, at least for such reasons, it is

believed that the rejection of such claims should be removed, and such action is respectfully requested.

Claim 11 was rejected under 35 USC § 103(a) as being unpatentable over Orchier in view of U.S. Pat. No. 5,958,012 (Battat). Such rejection assumes that reference Orchier was properly applied to the claims. However, for the reasons discussed above, it is believed that such application of Orchier was incorrect. Therefore, the rejection of claim 11 under 35 USC § 103(a) is believed incorrect. For example, as discussed above, it is believed that Orchier fails to teach display of status of network security devices and summary lines, said summary lines comprising hypertext links providing access to further data. Therefore, the removal of the rejection of claim 11 is respectfully requested.

Claim 16 was rejected under 35 USC § 103(a) as being unpatentable over Orchier in view of U.S. Pat. No. 6,088,804 (Hill). Such rejection assumes that Orchier was properly applied to the claims. However, it is believed that such application of Orchier was incorrect, for the reasons discussed above. Therefore, it is believed the rejection of claim 16 should be removed, and such action is respectfully requested.

Claims 23, 24 and 32 were rejected under 35 USC § 103(a) as being unpatentable over Orchier. Such rejection assumes that the prior application of Orchier to the claims in the Office Action was correct. However, for the reasons discussed above, it is believed that such application of Orchier was incorrect. Therefore, it is believed that the rejection of claims 23, 24 and 32 should be removed, and such action is respectfully requested.

Additional Amendment of Claims

Claims 3, 4, 25 and 27 have been amended to include "and" to connect cited elements. Such amendment is for the convenience of the reader and is not believed to change the meaning of the claims.

CONCLUSION

Applicants submit that the instant application is in condition for allowance. Should the Examiner have any questions, the Examiner is requested to contact the undersigned attorney.

The Commissioner is authorized to charge any additional fees which may be required, including petition fees and extension of time fees, to Deposit Account No. 23-2415 (Docket No. 26836.701.201).

Respectfully submitted,

WILSON SONSINI GOODRICH & ROSATI

Date: August 25, 2004

George A. Wilman, Reg. No. 41,378

650 Page Mill Road
Palo Alto, CA 94304
(650) 320-4945
Customer No. 021971